


**Content Types   Subject Collections**

Athens Authentication Point

**Recognized as:**

U.S. Patent & Trademark  
Office, Scientific & Technical  
(665-54-532)

US Patent and Trademark  
2007 3686.002  
(911-40-100)

**Welcome!**

To use the personalized  
features of this site, please  
**log in or register.**

If you have forgotten your  
username or password, we  
can **help**.

**My SpringerLink**

Marked Items

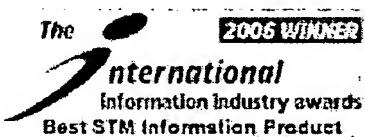
Alerts

Order History

**Saved Items**

All

Favorites

**Data Encryption**

REMOVE Search For (Boolean) > (homomorphism OR  
homomorphic) AND (abelian OR commutative) AND (signature OR  
hashing OR hash)  
REMOVE Subject > Data Encryption

Disable Highlighting

**Expanded View****Condensed View**182 Results First | 1-10 | **11-20** | 21-30 | 31-40 | 41-50 | Next

◀  Access to all content  Access to some content  
 Access to no content

11. Journal Article Add to marked items  
**The Round Functions of Cryptosystem PGM Generate the Symmetric Group**

DOI 10.1007/s10623-005-5667-z  
 Journal Designs, Codes and Cryptography  
 Issue Volume 38, Number 1 / January, 2006  
 Authors A. Caranti and F. Dalla. Volta  
 Subject Collection Mathematics and Statistics  
 Abstract ...et al. have described symmetric and public key cryptosystems based on logarithmic signatures (also known as group bases) for finite permutation groups  
 Text PDF (103 kb)  
 Rightslink Permissions & Reprints

12. Journal Article Add to marked items  
**A General Zero-Knowledge Scheme**

DOI 10.1023/A:1008237708202  
 Journal Designs, Codes and Cryptography  
 Issue Volume 12, Number 1 / September, 1997  
 Authors Mike Burmester, Yvo G. Desmedt, Fred Piper and Michael Walker  
 Subject Collection Mathematics and Statistics  
 Text PDF (5 kb)  
 Rightslink Permissions & Reprints

13. Journal Article Add to marked items  
**Identity-based key**

**Find**

(homomorp

Within i

Within t

**Starts Wit**a b c d e  
p q r s t**SpringerL**

In the last

In the last

In the last

**Content T**

Book Chap

Journal Art

**Subject**

Computer

Computer Networks (

Artificial In  
Robotics) (

Software E

Database F

Algorithm ,  
ComplexityComputatio  
(171)

Mathematic

Combinato

Data Struc  
Informatio**Copyright**

2007 (27)

2006 (31)

	agreement protocols from pairings	2004 (40)
Category	Regular Contribution	2003 (4)
DOI	10.1007/s10207-006-0011-9	2000 (12)
Journal	International Journal of Information Security	1999 (4)
Issue	Volume 6, Number 4 / July, 2007	1998 (8)
Authors	L. Chen, Z. Cheng and N. P. Smart	1997 (10)
Subject Collection	Computer Science	Publicatio
Text	PDF (534 kb) HTML	Lecture No
Rightslink	Permissions & Reprints	Science (1
<input checked="" type="checkbox"/> 14. Book Chapter	A Useful Undecidable Theory	Add to marked items
DOI	10.1007/978-3-540-73001-9_73	Author
Book Series	Lecture Notes in Computer Science	José Meseg
Volume	Volume 4497/2007	Ivan Damg
Book	Computation and Logic in the Real World	Serge Vau
Author	Victor L. Selivanov	Stéphanie
Subject Collection	Computer Science	Ronald Cra
Text	PDF (395 kb)	Hartmut El
<input checked="" type="checkbox"/> 15. Book Chapter	Functional Semantics of Rewrite Theories	Add to marked items
Category	Algebraic Specification and Logic	Huaxiong
Book Series	Lecture Notes in Computer Science	Paliath Nar
Volume	Volume 3393/2005	Franz Baac
Book	Formal Methods in Software and Systems Modeling	Alfred Men
Author	José Meseguer	
Subject Collection	Computer Science	
Text	PDF (222 kb)	
<input checked="" type="checkbox"/> 16. Book Chapter	Weak Fields for ECC	Add to marked items
Category	Elliptic Curve Cryptosystems	
Book Series	Lecture Notes in Computer Science	
Volume	Volume 2964/2004	
Book	Topics in Cryptology - CT-RSA 2004	
Authors	Alfred Menezes, Edlyn Teske and Ansgret Weng	
Subject Collection	Computer Science	

	Text	PDF (300 kb) HTML
17.	Book Chapter <b>Petri nets, process algebras and concurrent programming languages</b>  Category DOI Book Series Volume Book Authors Subject Collection Text	Add to marked items  IV Applications of Elementary Net Systems and Place/Transition Nets 10.1007/3-540-65307-4_46 Lecture Notes in Computer Science Volume 1492/1998 Lectures on Petri Nets II: Applications Eike Best, Raymond Devillers and Maciej Koutny Computer Science PDF (5,397 kb)
18.	Book Chapter <b>Analysis of a Multi-party Fair Exchange Protocol and Formal Proof of Correctness in the Strand Space Model</b>  Category DOI Book Series Volume Book Authors Subject Collection Text	Add to marked items  Exchanges and Contracts 10.1007/11507840_23 Lecture Notes in Computer Science Volume 3570/2005 Financial Cryptography and Data Security Aybek Mukhamedov, Steve Kremer and Eike Ritter Computer Science PDF (224 kb)
19.	Book Chapter <b>Verifiable Shuffle of Large Size Ciphertexts</b>  DOI Book Series Volume Book Authors Subject Collection Abstract	Add to marked items  10.1007/978-3-540-71677-8_25 Lecture Notes in Computer Science Volume 4450/2007 Public Key Cryptography – PKC 2007 Jens Groth and Steve Lu Computer Science ...correctness of a shuffle. We first suggest a HVZK argument based on homomorphic integer commitments, and improve both on round

		complexity, communication complexity and computational...
	Text	PDF (541 kb)
 20.	Book Chapter Algorithms to Speed Up Computations in Threshold RSA	Add to marked items
Category	Secret Sharing II	
DOI	10.1007/10718964_36	
Book Series	Lecture Notes in Computer Science	
Volume	Volume 1841/2000	
Book	Information Security and Privacy	
Author	Brian King	
Subject Collection	Computer Science	
Abstract	...Frankel described a threshold scheme which can be used with any finite abelian group. Hence it can be used to provide a threshold RSA scheme...	
Text	PDF (243 kb)	

182 Results First | 1-10 | **11-20** | 21-30 | 31-40 | 41-50 | Next

[Frequently asked questions](#) | [General information on journals and books](#) | [Send Impressum](#)

© Springer. Part of Springer Science+Business Media

[Privacy](#), [Disclaimer](#), [Terms and Conditions](#), © Copyright Information

Remote Address: 151.207.242.4 • Server: mpweb20

HTTP User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1; .NET CLR 2.0.50727)



Athens Authentication Point

**Recognized as:**U.S. Patent & Trademark  
Office, Scientific & Technical  
(665-54-532)US Patent and Trademark  
2007 3686.002  
(911-40-100)**Welcome!**To use the personalized  
features of this site, please  
**log in or register.**If you have forgotten your  
username or password, we  
can **help**.**My SpringerLink**

Marked Items

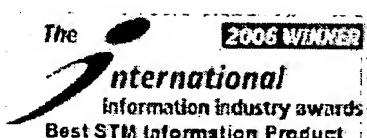
Alerts

Order History

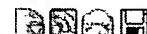
**Saved Items**

All

Favorites

**Content Types Subject Collections****Data Encryption**REMOVE Search For (Boolean) > "group  
homomorphism" AND (signature OR hash OR hashing)  
REMOVE Subject > Data Encryption

Disable Highlighting

**Expanded View****Condensed View**37 Results First | **1-10** | 11-20 | 21-30 | 31-37 | Next

Access to all content  
  Access to some content  
  Access to no content

1. Book Chapter  
**On Pairing** Add to marked items  
**Inversion Problems**

DOI 10.1007/978-3-540-73489-5\_18

Book Series Lecture Notes in  
Computer Science

Volume Volume 4575/2007

Book Pairing-Based  
Cryptography –  
Pairing 2007

Author Takakazu Satoh

Subject Collection Computer Science

Text PDF (453 kb)

2. Book Chapter  
**Efficient Zero-** Add to marked items  
**Knowledge Proofs of Knowledge**  
**without Intractability Assumptions**

Book Series Lecture Notes in  
Computer Science

Volume Volume 1751/2004

Book Public Key  
CryptographyAuthors Ronald Cramer, Ivan  
Damgård and Philip  
MacKenzie

Subject Collection Computer Science

Text PDF (354 kb)

3. Book Chapter  
**Cryptographic** Add to marked items  
**Asynchronous Multi-party**  
**Computation with Optimal**  
**Resilience (Extended Abstract)**

Category Secure Protocols

**Find** "group homomorphism" Within all content Within these results**Starts With** a b c d e f g h i j  
 p q r s t u v w x y**SpringerLink Date**

In the last six months

In the last year (9)

**Content Type**

Book Chapters (35)

Journal Articles (2)

**Subject**

Computer Science (1)

Computer Communications  
Networks (36)Artificial Intelligence  
Robotics) (35)Software Engineering  
Database ManagementAlgorithm Analysis and  
Complexity (35)Computation by Abstract  
(35)

Mathematics (1)

Management of Computer  
Information SystemsData Structures, Cryptography  
Information Theory (1)**Copyright**

2007 (6)

2006 (4)

2005 (10)

2004 (10)

DOI	10.1007/11426639_19	2000 (1)
Book Series	Lecture Notes in Computer Science	1999 (1)
Volume	Volume 3494/2005	1998 (5)
Book	Advances in Cryptology – EUROCRYPT 2005	<b>Publication</b>
Authors	Martin Hirt, Jesper Buus Nielsen and Bartosz Przydatek	Lecture Notes in Computer Science (35)
Subject Collection	Computer Science	Designs, Codes and
Text	PDF (277 kb)	(1)
		International Journal of Information Security
<input type="checkbox"/> 4.	Book Chapter Cryptanalysis of Two Anonymous Buyer-Seller Watermarking Protocols and an Improvement for True Anonymity	Add to marked items
Category	Cryptographic Protocols	<b>Author</b>
Book Series	Lecture Notes in Computer Science	Tsuyoshi Takagi
Volume	Volume 3089/2004	Ivan Damgård
Book	Applied Cryptography and Network Security	Feng Bao
Authors	Bok-Min Goi, Raphael C.-W. Phan, Yanjiang Yang, Feng Bao, Robert H. Deng and M.U. Siddiqi	Maurice Herlihy
Subject Collection	Computer Science	Takakazu Satoh
Text	PDF (188 kb)	Katja Schmidt-Samc
		Sergio Rajsbaum
<input type="checkbox"/> 5.	Book Chapter Homomorphic Cryptosystems Based on Subgroup Membership Problems	Add to marked items
Category	Homomorphic Encryption	
DOI	10.1007/11554868_22	
Book Series	Lecture Notes in Computer Science	
Volume	Volume 3715/2005	
Book	Progress in Cryptology – Mycrypt 2005	
Author	Kristian Gjøsteen	
Subject Collection	Computer Science	
Text	PDF (219 kb)	
<input type="checkbox"/> 6.	Book Chapter Efficient Strongly Universal and Optimally Universal	Add to marked items

	Hashing	
	Extended Abstract	
DOI	10.1007/3-540-48340-3_24	
Book Series	Lecture Notes in Computer Science	
Volume	Volume 1672/1999	
Book	Mathematical Foundations of Computer Science 1999	
Author	Philipp Woelfel	
Subject Collection	Computer Science	
Abstract	New hash families are analyzed, mainly consisting of the hash functions h <sub>a,b...</sub>	
Text	PDF (594 kb)	
<input type="checkbox"/> 7.	Book Chapter Cryptanalysis of Two Non-anonymous Buyer-Seller Watermarking Protocols for Content Protection	Add to marked items
	DOI	10.1007/978-3-540-74472-6_77
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 4705/2007
	Book	Computational Science and Its Applications – ICCSA 2007
	Authors	Bok-Min Goi, Raphael C. -W. Phan and Hean-Teik Chuah
	Subject Collection	Computer Science
	Text	PDF (442 kb)
<input type="checkbox"/> 8.	Book Chapter Reducing Logarithms in Totally Non-maximal Imaginary Quadratic Orders to Logarithms in Finite Fields	Add to marked items
	Category	Integers and Computation
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 1716/2004
	Book	Advances in Cryptology - ASIACRYPT'99

Authors	Detlef Hühnlein and Tsuyoshi Takagi
Subject Collection	Computer Science
Text	PDF (220 kb)
<hr/>	
<input type="checkbox"/> 9. Book Chapter	Add to marked items
Efficient Private Matching and Set Intersection	
Book Series	Lecture Notes in Computer Science
Volume	Volume 3027/2004
Book	Advances in Cryptology - EUROCRYPT 2004
Authors	Michael J. Freedman, Kobbi Nissim and Benny Pinkas
Subject Collection	Computer Science
Abstract	...We present protocols, based on the use of homomorphic encryption and balanced hashing, for both semi-honest and malicious environments. For lists of length k...
Text	PDF (326 kb)
<hr/>	
<input type="checkbox"/> 10. Book Chapter	Add to marked items
Cryptography, Connections, Cocycles and Crystals: A p-Adic Exploration of the Discrete Logarithm Problem	
Category	Public Key Cryptanalysis
Book Series	Lecture Notes in Computer Science
Volume	Volume 3348/2004
Book	Progress in Cryptology - INDOCRYPT 2004
Authors	H. Gopalkrishna Gadiyar, K. M. Sangeeta Maini and R. Padma
Subject Collection	Computer Science
Text	PDF (147 kb)

37 Results [First](#) | **1-10** | 11-20 | 21-30 | 31-37 | [Next](#)

[Privacy, Disclaimer, Terms and Conditions, © Copyright Information](#)

Remote Address: 151.207.242.4 • Server: mpweb04  
HTTP User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1; .NET CLR 2.0.50529.3019)


**Content Types   Subject Collections**

Athens Authentication Point

**Recognized as:**

U.S. Patent & Trademark  
Office, Scientific & Technical  
(665-54-532)

US Patent and Trademark  
2007 3686.002  
(911-40-100)

**Welcome!**

To use the personalized  
features of this site, please  
**log in or register.**

If you have forgotten your  
username or password, we  
can **help**.

**My SpringerLink**

Marked Items

Alerts

Order History

**Saved Items**

All

Favorites

**Data Encryption**

REMOVE Search For (Boolean) > "group homomorphism"  
AND (signature OR hash OR hashing)  
REMOVE Subject > Data Encryption

**Find**

"group homomorphism"

Within all content

Within these results

Disable Highlighting

**Expanded View****Condensed View**37 Results First | 1-10 | **11-20** | 21-30 | 31-37 | Next

Access to all content  
 Access to some content  
 Access to no content

<input type="checkbox"/>	<b>11.</b> Journal Article The Round Functions of Cryptosystem PGM Generate the Symmetric Group	Add to marked items
	DOI	10.1007/s10623-005-5667-z
	Journal	Designs, Codes and Cryptography
	Issue	Volume 38, Number 1 / January, 2006
	Authors	A. Caranti and F. Dalla. Volta
	Subject Collection	Mathematics and Statistics
	Abstract	...et al. have described symmetric and public key cryptosystems based on logarithmic signatures (also known as group bases) for finite permutation groups
	Text	PDF (103 kb)
	Rightslink	Permissions & Reprints

<input type="checkbox"/>	<b>12.</b> Journal Article Identity-based key agreement protocols from pairings	Add to marked items
	Category	Regular Contribution
	DOI	10.1007/s10207-006-0011-9
	Journal	International Journal of Information Security
	Issue	Volume 6, Number 4 / July, 2007

**Starts With**

a b c d e f g h i  
p q r s t u v w x

**SpringerLink Date**

In the last six months

In the last year (9)

**Content Type**

Book Chapters (35)

Journal Articles (2)

**Subject**

Computer Science (1)

Computer Communications and Networks (36)

Artificial Intelligence and Robotics (35)

Software Engineering (1)

Database Management (1)

Algorithm Analysis and Complexity (35)

Computation by Abstract (35)

Mathematics (1)

Management of Computer Information Systems (1)

Data Structures, Cryptography and Information Theory (1)

**Copyright**

2007 (6)

2006 (4)

2005 (10)

2004 (10)

	Authors	L. Chen, Z. Cheng and N. P. Smart	2000 (1)
	Subject Collection	Computer Science	1999 (1)
	Text	PDF (534 kb) HTML	1998 (5)
	Rightslink	Permissions & Reprints	<b>Publication</b>
<input type="checkbox"/> 13.	Book Chapter Two-Party Privacy- Preserving Agglomerative Document Clustering	Add to marked items	Lecture Notes in Cor Science (35) Designs, Codes and (1) International Journa Information Security
	DOI	10.1007/978-3-540- 72163-5_16	
	Book Series	Lecture Notes in Computer Science	<b>Author</b>
	Volume	Volume 4464/2007	Tsuyoshi Takagi
	Book	Information Security Practice and Experience	Serge Vaudenay
	Authors	Chunhua Su, Jianying Zhou, Feng Bao, Tsuyoshi Takagi and Kouichi Sakurai	Jean Monnerat
	Subject Collection	Computer Science	Ronald Cramer
	Text	PDF (412 kb)	Ivan Damgård
<input checked="" type="checkbox"/> 14.	Book Chapter Weak Fields for ECC	Add to marked items	Feng Bao
	Category	Ellictic Curve Cryptosystems	Maurice Herlihy
	Book Series	Lecture Notes in Computer Science	Takakazu Satoh
	Volume	Volume 2964/2004	
	Book	Topics in Cryptology - CT-RSA 2004	Katja Schmidt-Samc
	Authors	Alfred Menezes, Edlyn Teske and Annegret Weng	Sergio Rajsbaum
	Subject Collection	Computer Science	
	Text	PDF (300 kb) HTML	
<input type="checkbox"/> 15.	Book Chapter Generic Homomorphic Undeniable Signatures	Add to marked items	
	Category	Digital Signatures	
	Book Series	Lecture Notes in Computer Science	
	Volume	Volume 3329/2004	
	Book	Advances in Cryptology - ASIACRYPT 2004	
	Authors	Jean Monnerat and	

	Subject Collection	Serge Vaudenay
	Abstract	Computer Science
		...that we transform a private group homomorphism from public groups G...being public) into an undeniable signature scheme. It is provably secure...
	Text	PDF (241 kb)
<input checked="" type="checkbox"/> 16.	Book Chapter <b>Custodian-Hiding Verifiable Encryption</b>	Add to marked items
	Category	Public Key Schemes I
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 3325/2005
	Book	Information Security Applications
	Authors	Joseph K. Liu, Victor K. Wei and Duncan S. Wong
	Subject Collection	Computer Science
	Text	PDF (208 kb)
<input checked="" type="checkbox"/> 17.	Book Chapter <b>Pairing-Friendly Elliptic Curves of Prime Order</b>	Add to marked items
	Category	Efficient Implementations
	DOI	10.1007/11693383_22
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 3897/2006
	Book	Selected Areas in Cryptography
	Authors	Paulo S.L.M. Barreto and Michael Naehrig
	Subject Collection	Computer Science
	Text	PDF (450 kb)
<input type="checkbox"/> 18.	Book Chapter <b>Factorization- Based Fail-Stop Signatures Revisited.</b>	Add to marked items
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 3269/2004
	Book	Information and Communications Security

Author	Katja Schmidt-Samoa
Subject Collection	Computer Science
Abstract	Fail-stop signature (FSS) schemes are important primitives because in a fail-stop signature scheme...
Text	PDF (2,137 kb)
<input type="checkbox"/> 19. Book Chapter	Add to marked items
<b>Paillier's Cryptosystem Modulo <math>p^2 q</math> and Its Applications to Trapdoor Commitment Schemes</b>	
Category	Homomorphic Encryption
DOI	10.1007/11554868_21
Book Series	Lecture Notes in Computer Science
Volume	Volume 3715/2005
Book	Progress in Cryptology - Mycrypt 2005
Authors	Katja Schmidt-Samoa and Tsuyoshi Takagi
Subject Collection	Computer Science
Abstract	...Tauman on-line/off-line signatures. Keywords: homomorphic encryption, trapdoor commitments, trapdoor hash families, on-line/off-line...
Text	PDF (287 kb)
<input type="checkbox"/> 20. Book Chapter	Add to marked items
<b>Fast Bilinear Maps from the Tate-Lichtenbaum Pairing on Hyperelliptic Curves</b>	
Category	Curves over Finite Fields and Applications
DOI	10.1007/11792086_33
Book Series	Lecture Notes in Computer Science
Volume	Volume 4076/2006
Book	Algorithmic Number Theory
Authors	Gerhard Frey and Tanja Lange
Subject Collection	Computer Science
Abstract	...also as a building block for

cryptosystems with special properties like short signatures or identity based encryption. In this paper we consider the Tate pairing...

Text

PDF (485 kb)

---

37 Results First | 1-10 | **11-20** | 21-30 | 31-37 | Next

[Frequently asked questions](#) | [General information on journals and books](#) | [Send feedback](#) | [Impressum](#)

© Springer. Part of Springer Science+Business Media

[Privacy](#); [Disclaimer](#), [Terms and Conditions](#), © Copyright Information

Remote Address: 151.207.242.4 • Server: mpweb19  
HTTP User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1; .NET CLR 2.0.50727.1432)


[Content Types](#) [Subject Collections](#)

Athens Authentication Point

**Recognized as:**

U.S. Patent & Trademark  
Office, Scientific & Technical  
(665-54-532)

US Patent and Trademark  
2007 3686.002  
(911-40-100)

**Welcome!**

To use the personalized  
features of this site, please  
[log in](#) or [register](#).

If you have forgotten your  
username or password, we  
can [help](#).

**My SpringerLink**[Marked Items](#)[Alerts](#)[Order History](#)**Saved Items**[All](#)[Favorites](#)**Data Encryption**

REMOVE Search For (Boolean) > "group homomorphism"  
AND (signature OR hash OR hashing)  
REMOVE Subject > Data Encryption

[Find](#)["group homomorphism"](#)[Within all content](#)[Within these results](#)[Disable Highlighting](#)[Expanded View](#)[Condensed View](#)37 Results First | 1-10 | 11-20 | **21-30** | 31-37 | Next

◀  Access to all content  
 Access to some content  
 Access to no content

21. Book Chapter  
 A wait-free  
 classification of loop agreement  
 tasks  
 Extended abstract

[Add to marked items](#)

Category

Contributed Papers

DOI

10.1007/BFb0056482

Book Series

Lecture Notes in

Computer Science

Volume 1499/1998

Volume

Volume 1499/1998

Book

Distributed

Authors

Computing

Maurice Herlihy and

Sergio Rajsbaum

Subject Collection

Computer Science

Abstract

...can be assigned an

algebraic signature

consisting of a

finitely-

presented...only if

there exists a group

homomorphism  $\Phi: G$  $\rightarrow H$  carrying...

Text

PDF (757 kb)

22. Book Chapter  
 Undeniable  
 Signatures Based on Characters:  
 How to Sign with One Bit

[Add to marked items](#)

Book Series

Lecture Notes in

Computer Science

Volume

Volume 2947/2004

Book

Public Key

Cryptography – PKC

2004

Authors

Jean Monnerat and

Serge Vaudenay

**Starts With**

a b c d e f g h i  
 p q r s t u v w x

**SpringerLink Date**

In the last six months

In the last year (9)

**Content Type**

Book Chapters (35)

Journal Articles (2)

**Subject**

Computer Science (35)

Computer Communications (36)

Artificial Intelligence (35)

Software Engineering (35)

Database Management (35)

Algorithm Analysis and Complexity (35)

Computation by Abstract (35)

Mathematics (1)

Management of Computer Information Systems (35)

Data Structures, Cryptography and Information Theory (35)

**Copyright**

2007 (6)

2006 (4)

2005 (10)

2004 (10)

	Subject Collection	Computer Science	2000 (1)
	Abstract	We present a new undeniable signature scheme which is based on the computation of characters. Our signature scheme...	1999 (1)
			1998 (5)
			<b>Publication</b>
	Text	PDF (306 kb) HTML	Lecture Notes in Computer Science (35)
<input checked="" type="checkbox"/> 23.	Book Chapter Implementing Cryptographic Pairings over Barreto-Naehrig Curves	Add to marked items	Designs, Codes and (1) International Journal of Information Security
	DOI	10.1007/978-3-540-73489-5_10	<b>Author</b>
	Book Series	Lecture Notes in Computer Science	Tsuyoshi Takagi
	Volume	Volume 4575/2007	Serge Vaudenay
	Book	Pairing-Based Cryptography – Pairing 2007	Jean Monnerat
	Authors	Augusto Jun Devegili, Michael Scott and Ricardo Dahab	Ronald Cramer
	Subject Collection	Computer Science	Ivan Damgård
	Text	PDF (422 kb)	Feng Bao
			Maurice Herlihy
			Takakazu Satoh
			Katja Schmidt-Samoa
			Sergio Rajsbaum
<input checked="" type="checkbox"/> 24.	Book Chapter Overview of elliptic curve cryptography	Add to marked items	
	DOI	10.1007/BFb0054012	
	Book Series	Lecture Notes in Computer Science	
	Volume	Volume 1431/1998	
	Book	Public Key Cryptography	
	Authors	Kiyomichi Araki, Takakazu Satoh and Shinji Miura	
	Subject Collection	Computer Science	
	Text	PDF (1,205 kb)	
<input checked="" type="checkbox"/> 25.	Book Chapter A Wait-Free Classification of Loop Agreement Tasks (Extended Abstract)	Add to marked items	
	Book Series	Lecture Notes in Computer Science	
	Volume	Volume 1499/1998	
	Book	Distributed Computing	

Authors	Maurice Herlihy and Sergio Rajsbaum
Subject Collection	Computer Science
Abstract	...can be assigned an algebraic signature consisting of a finitely-presented...only if there exists a group homomorphism $\Phi : G \rightarrow H$ ...
Text	PDF (570 kb)
<b>26.</b>  Book Chapter Optimization of the MOVA Undeniable Signature Scheme	Add to marked items
Category	Implementation Issues
DOI	10.1007/11554868_14
Book Series	Lecture Notes in Computer Science
Volume	Volume 3715/2005
Book	Progress in Cryptology - Mycrypt 2005
Authors	Jean Monnerat, Yvonne Anne Oswald and Serge Vaudenay
Subject Collection	Computer Science
Abstract	...results on the MOVA undeniable signature scheme presented last year by...is based on a secret group homomorphism. The original MOVA scheme...
Text	PDF (240 kb)
<b>27.</b>  Book Chapter A New Cramer-Shoup Like Methodology for Group Based Provably Secure Encryption Schemes	Add to marked items
Category	Encryption and Signatures
Book Series	Lecture Notes in Computer Science
Volume	Volume 3378/2005
Book	Theory of Cryptography
Authors	María Isabel González Vasco, Consuelo Martínez, Rainer Steinwandt

	Subject Collection	and Jorge L. Villar
	Text	Computer Science
		PDF (219 kb)
<input type="checkbox"/> 28.	Book Chapter	Add to marked items
	Zero-knowledge proofs for finite field arithmetic, or: Can zero-knowledge be for free?	
	DOI	10.1007/BFb0055745
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 1462/1998
	Book	Advances in Cryptology — CRYPTO '98
	Authors	Ronald Cramer and Ivan Damgård
	Subject Collection	Computer Science
	Text	PDF (1,132 kb)
<input type="checkbox"/> 29.	Book Chapter	Add to marked items
	2 RSA and Probabilistic Prime Number Tests	
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 3028/2004
	Book	Probabilistic and Statistical Methods in Cryptology
	Author	Daniel Neuenschwander
	Subject Collection	Computer Science
	Text	PDF (274 kb)
<input type="checkbox"/> 30.	Book Chapter	Add to marked items
	Pairings on Elliptic Curves over Finite Commutative Rings	
	Category	Number Theoretic Foundations
	DOI	10.1007/11586821_26
	Book Series	Lecture Notes in Computer Science
	Volume	Volume 3796/2005
	Book	Cryptography and Coding
	Authors	Steven D. Galbraith and James F. McKee
	Subject Collection	Computer Science
	Text	PDF (265 kb)

37 Results First | 1-10 | 11-20 | 21-30 | 31-37 | Next

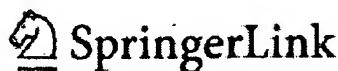
[Frequently asked questions](#) | [General information on journals and books](#) | [Send us your feedback](#)

[feedback](#) | [Impressum](#)

© Springer. Part of Springer Science+Business Media

[Privacy](#), [Disclaimer](#), [Terms and Conditions](#), © Copyright Information

• Remote Address: 151.207.242.4 • Server: mpweb22  
HTTP User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1; .NET CLR 2.0.50522)



Athens Authentication Point

**Recognized as:**U.S. Patent & Trademark  
Office, Scientific & Technical  
(665-54-532)US Patent and Trademark  
2007 3686.002  
(911-40-100)**Welcome!**To use the personalized  
features of this site, please  
**log in or register.**If you have forgotten your  
username or password, we  
can **help**.**My SpringerLink**

Marked Items

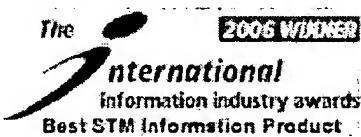
Alerts

Order History

**Saved Items**

All

Favorites

**Content Types   Subject Collections****Data Encryption**REMOVE Search For (Boolean) > "group homomorphism"  
AND (signature OR hash OR hashing)  
REMOVE Subject > Data Encryption**Find** "group homomorphism" Within all content Within these results

Disable Highlighting

**Expanded View****Condensed View**37 Results First | 1-10 | 11-20 | 21-30 | **31-37** | Next

◀  Access to all content  
 Access to some content  
 Access to no content

31. Book Chapter Add to marked items  
 Upper Bounds on the Communication Complexity of Optimally Resilient Cryptographic Multiparty Computation

Category	Multiparty Computation	<b>Content Type</b> Book Chapters (35) Journal Articles (2)
DOI	10.1007/11593447_5	
Book Series	Lecture Notes in Computer Science	
Volume	Volume 3788/2005	
Book	Advances in Cryptology - ASIACRYPT 2005	
Authors	Martin Hirt and Jesper Buus Nielsen	
Subject Collection	Computer Science	<b>Subject</b> Computer Science (35) Computer Communications and Networks (36) Artificial Intelligence and Robotics (35) Software Engineering (35) Database Management (35) Algorithm Analysis and Computational Complexity (35) Computation by Abstract Methods (35) Mathematics (1) Management of Computer Information Systems (35) Data Structures, Cryptology and Information Theory (35)
Text	PDF (301 kb)	

32. Book Chapter Add to marked items  
 On Multiplicative Secret Sharing Schemes

Category	Secret Sharing I	<b>Copyright</b> 2007 (6)
DOI	10.1007/10718964_28	
Book Series	Lecture Notes in Computer Science	
Volume	Volume 1841/2000	
Book	Information Security and Privacy	
Authors	Huaxiong Wang, Kwok Yan Lam, Guo-Zhen Xiao and Huanhui Zhao	
Subject Collection	Computer Science	<b>2006 (4)</b>
Abstract	...such as in threshold RSA signature schemes. In this paper	2005 (10)
		2004 (10)

**Starts With**a b c d e f g h i j  
p q r s t u v w x y z**SpringerLink Date**

In the last six months

In the last year (9)

**Content Type**Book Chapters (35)  
Journal Articles (2)**Subject**Computer Science (35)  
Computer Communications and Networks (36)  
Artificial Intelligence and Robotics (35)  
Software Engineering (35)  
Database Management (35)  
Algorithm Analysis and Computational Complexity (35)  
Computation by Abstract Methods (35)  
Mathematics (1)  
Management of Computer Information Systems (35)  
Data Structures, Cryptology and Information Theory (35)**Copyright**2007 (6)  
2006 (4)  
2005 (10)  
2004 (10)

		we...a notion of multiple perfect hash families, which we introduce in...	2000 (1)
		PDF (142 kb)	1999 (1)
			1998 (5)
			<b>Publication</b>
<input type="checkbox"/>	<b>33.</b>	Book Chapter Optimistic fair exchange of digital signatures Extended abstract	Add to marked items
		DOI	10.1007/BFb0054156
		Book Series	Lecture Notes in Computer Science
		Volume	Volume 1403/1998
		Book	Advances in Cryptology — EUROCRYPT'98
		Authors	N. Asokan, Victor Shoup and Michael Waidner
		Subject Collection	Computer Science
		Abstract	We present a new protocol that allows two players to exchange digital signatures over the Internet in a fair way, so that either each player...
		Text	PDF (895 kb)
			<b>Author</b>
			Tsuyoshi Takagi
			Serge Vaudenay
			Jean Monnerat
			Ronald Cramer
			Ivan Damgård
			Feng Bao
			Maurice Herlihy
			Takakazu Satoh
			Katja Schmidt-Samoa
			Sergio Rajsbaum
<input type="checkbox"/>	<b>34.</b>	Book Chapter Efficient Proofs of Knowledge of Discrete Logarithms and Representations in Groups with Hidden Order	Add to marked items
		Category	Building Blocks
		Book Series	Lecture Notes in Computer Science
		Volume	Volume 3386/2005
		Book	Public Key Cryptography - PKC 2005
		Authors	Endre Bangerter, Jan Camenisch and Ueli Maurer
		Subject Collection	Computer Science
		Text	PDF (272 kb)
<input type="checkbox"/>	<b>35.</b>	Book Chapter Do All Elliptic Curves of the Same Order Have the Same Difficulty of Discrete Log?	Add to marked items

Category	Algebra and Number Theory
DOI	10.1007/11593447_2
Book Series	Lecture Notes in Computer Science
Volume	Volume 3788/2005
Book	Advances in Cryptology - ASIACRYPT 2005
Authors	David Jao, Stephen D. Miller and Ramarathnam Venkatesan
Subject Collection	Computer Science
Text	PDF (562 kb)
<b>36.</b>	<b>Book Chapter</b> <b>Definability in the Homomorphic Quasiorder of Finite Labeled Forests</b>
DOI	10.1007/978-3-540-73001-9_45
Book Series	Lecture Notes in Computer Science
Volume	Volume 4497/2007
Book	Computation and Logic in the Real World
Authors	Oleg V. Kudinov and Victor L. Selivanov
Subject Collection	Computer Science
Text	PDF (410 kb)
<b>37.</b>	<b>Book Chapter</b> <b>Short 2-Move Undeniable Signatures</b>
Category	Signatures and Lightweight Cryptography
DOI	10.1007/11958239_2
Book Series	Lecture Notes in Computer Science
Volume	Volume 4341/2006
Book	Progress in Cryptology - VIETCRYPT 2006
Authors	Jean Monnerat and Serge Vaudenay
Subject Collection	Computer Science
Abstract	...we offer a solution to this problem in the context of undeniable signatures with interactive verification protocols

by proposing a way  
to achieve these  
protocols...

Text

PDF (596 kb)

---

37 Results | First | 1-10 | 11-20 | 21-30 | **31-37** | Next

[Frequently asked questions](#) | [General information on journals and books](#) | [Send feedback](#) | [Impressum](#)

© Springer. Part of Springer Science+Business Media

[Privacy](#), [Disclaimer](#), [Terms and Conditions](#), © Copyright Information

Remote Address: 151.207.242.4 • Server: mpweb18

HTTP User Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1; InfoPath.1; .NET CLR 2.0.50524.1)

# Dialog DataStar

[options](#)[logoff](#)[tracker](#)[feedback](#)[help](#)

## Advanced Search: Examiners' Electronic Digest Database (EEDD)

[limit](#)

Search history:

No.	Database	Search term	Results	
CP		[Clipboard]	0	-
1	EEDD	group ADJ homomorphism	0	-
2	EEDD	homomorphism	0	-
3	EEDD	abelian AND hash	0	-
4	EEDD	abelian AND signature	0	-

[hide](#) | [delete all search steps...](#) | [delete individual search steps...](#)Enter your search term(s): [Search tips](#) whole document[search](#) Documents available in fulltext

Select special search terms from the following list(s):

 Document type[Top - News & FAQS - Dialog](#)

© 2007 Dialog

[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase His](#)

Welcome United States Patent and Trademark Office

 [Search Results](#)[BROWSE](#)[SEARCH](#)[IEEE Xplore GUIDE](#)

Results for "((group homomorphism &lt;and&gt; signature)&lt;in&gt;metadata)"

Your search matched 0 of 1692897 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by Relevance in Descending order.

[Modify Search](#) Check to search only within this results set

Display Format:

 Citation Citation & Abstract[» Search Options](#)[IEEE/IET](#)[Books](#)[Educational Courses](#)[IEEE/IET journals, transactions, letters, magazines, conference proceedings, and standards.](#)[Select All](#) [Deselect All](#)[» Key](#)

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

No results were found.

Please edit your search criteria and try again. Refer to the Help pages if you need assistance revising your search

[Help](#) [Contact](#)[Copy](#)

[Home](#) | [Login](#) | [Logout](#) | [Access Information](#) | [Alerts](#) | [Purchase Help](#)

Welcome United States Patent and Trademark Office

 [Search Results](#)[BROWSE](#)[SEARCH](#)[IEEE Xplore GUIDE](#)

Results for "((homomorphism &lt;and&gt; signature)&lt;in&gt;metadata)"

Your search matched 3 of 1692897 documents.

A maximum of 100 results are displayed, 25 to a page, sorted by **Relevance** in **Descending** order.[Modify Search](#) [Check to search only within this results set](#)

Display Format:

 [Citation](#) [Citation & Abstract](#)[» Search Options](#)[View Session History](#)[New Search](#)[IEEE/IEET](#)[Books](#)[Educational Courses](#)[IEEE/IEET journals, transactions, letters, magazines, conference proceedings, and standards.](#)[» Key](#)

IEEE JNL	IEEE Journal or Magazine
IET JNL	IET Journal or Magazine
IEEE CNF	IEEE Conference Proceeding
IET CNF	IET Conference Proceeding
IEEE STD	IEEE Standard

[Select All](#) [Deselect All](#)

1. **Signature scheme based on discrete logarithm without using one-way hash-function**  
Yeun, C.Y.; Mitchell, C.J.; Ng, S.L.;  
[Electronics Letters](#)  
Volume 34, Issue 24, 26 Nov. 1998 Page(s):2329 - 2330  
[AbstractPlus](#) | Full Text: [PDF\(236 KB\)](#) IET JNL

2. **Signature scheme based on discrete logarithm without using one-way hash function**  
Zuhua Shao;  
[Electronics Letters](#)  
Volume 34, Issue 11, 28 May 1998 Page(s):1079 - 1080  
[AbstractPlus](#) | Full Text: [PDF\(248 KB\)](#) IET JNL

3. **Parsing languages by pattern matching**  
Rus, T.;  
[Software Engineering, IEEE Transactions on](#)  
Volume 14, Issue 4, Apr 1988 Page(s):498 - 511  
Digital Object Identifier 10.1109/32.4672  
[AbstractPlus](#) | Full Text: [PDF\(1284 KB\)](#) IEEE JNL  
[Rights and Permissions](#)

Indexed by  
 Inspec

[Help](#) [Contact](#)[Copy](#)